Calculating Security Return on Investment

Don O'Neill, Software Engineering Institute [vita[1]]

2007-02-06 L1 / L, M[2]

With the dramatic increase in cyberspace incidents and perceptions about the high cost of security readiness and survivability, there is a need for a method to reason about and compute security return on investment (ROI). This article describes several such methods.

Overview

Security return on investment (ROI) has been difficult to calculate successfully. In the absence of actual data on the number of incidents, organizations are often forced to make estimates. Also, the impact of an individual incident can be difficult to assess. In spite of those drawbacks, a common industry security ROI method would deliver several benefits, including the following:

- The contributors to security readiness, the costs to achieve security readiness, and the costs to recover from cyberspace incidents can be better understood.
- The enterprise can reason about its security investment decision with increased precision.
- The public-private collaboration discussion on who is responsible for paying for security can be better informed.
- The relationship between levels of security readiness and recovery costs can contribute to the actuarial basis for underwriting cyberspace insurance.
- The state of security readiness for the nation's critical infrastructure dependent on software can be better assessed.

In this article, we describe several ways to compute security ROI. The ROI that we discuss is based on the aggregated security infrastructure. Further work is needed to calculate the ROI associated with adding a single security mechanism. Other methods for calculating ROI exist in the literature as well; see for instance *Estimating Benefits from Investing in Secure Software Development* [Arora 05[4]] and "Measuring the Risk Based Value of IT Security Solutions" [Arora 04[5]].

Expressing Security Return on Investment

Security ROI is savings divided by cost. Reasoning about ROI, then, is assisted by evaluating the expression [ROI: = Savings/Cost] where

- ***Savings*** is cost avoidance resulting from resistance, recognition, and reconstitution efforts.
- ***Cost*** includes preparation and incident cost. Incident cost is cleanup, lost opportunity, and critical infrastructure impact.

Methods for computing security ROI are needed to answer questions important to the security investment decision, such as the following:

- If the expected number of incidents is low, will the security readiness investment be recouped?
- For a higher number of cyber attack incidents, what are the minimum factors needed to fully recoup security investment?
- Is there an equitable scheme for sharing security readiness costs among the project, the enterprise, and the government?

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/681-BSI.html (O'Neill, Don)
4. #dsy677-BSI_arora05
5. #dsy677-BSI_arora04

- What are the guidelines for public-private collaboration and cost sharing?

There are methods for computing savings and cost. The values used in the expressions for these methods must be realistic, accurate, and tailored to the enterprise operation. Consider the following methods:

ROI #1
Savings: = (Resistance Savings + Recognition Savings + Reconstitution Savings)
Cost: = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical Infrastructure Impact)

ROI #2
Savings: = (Full Cost Incurred # Cost with Avoidance)
Cost: = (Preparation + Cost with Avoidance)

ROI #3
Savings: = (Full Cost Incurred)
Cost: = (Preparation + Cost with Avoidance)

Definition of Terms Common to ROI # 1, ROI #2, and ROI #3

Defining the terms common to all three of these security ROI expressions, fully delineates them for each one (i.e., for ROI #1, ROI #2, and ROI #3).

Cost: = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical Infrastructure Impact)

Where:
Incidents: = Expected number of incidents
IR1: Number of expected incidents successfully resisted
IR2: Number of expected incidents successfully recognized
IR3: Number of expected incidents successfully survived
IR4: Number of expected incidents undetected (duds) except for a forensic trace

Preparation
Step 1: = Awareness & Commitment [number of days * number of participants * cost per day]
Step 2: = Basic Practices Training [number of days * number of participants * cost per day]
Step 3: = Resistance and Recognition implementation costs
Step 4: = Reconstitution implementation costs
Step 5: = Information disclosure control costs
Total Preparation: = (Step1 + Step2 + Step3 + Step4 + Step5)

Cleanup per Incident
Cleanup1: = Cost/incident for incidents successfully resisted
Cleanup2: = Cost/incident for incidents successfully recognized
Cleanup3: = Cost/incident for incidents successfully survived
Cleanup4: = Cost/incident for incidents undetected (duds) except for a forensic trace
Total Cleanup: = (IR1 * Cleanup1) + (IR2 * Cleanup2) + (IR3 * Cleanup3) + (IR4 * Cleanup4)

Lost Opportunity per Incident
Lost Opportunity1: = number of days * lost opportunity cost/day for incidents successfully resisted
Lost Opportunity2: = number of days * lost opportunity cost/day for incidents successfully recognized
Lost Opportunity3: = number of days * lost opportunity cost/day for incidents successfully survived
Total Lost Opportunity: = (IR1 * Lost Opportunity1) + (IR2 * Lost Opportunity2) + (IR3 * Lost Opportunity3)

Critical Infrastructure Impact per Incident
Critical Infrastructure Impact1: = number of days * lost opportunity cost/day for incidents successfully resisted
Critical Infrastructure Impact2: = number of days * lost opportunity cost/day for incidents successfully recognized
Critical Infrastructure Impact3: = number of days * lost opportunity cost/day for incidents successfully survived

Total Critical Infrastructure Impact: = (IR1 * Critical Infrastructure Impact1) + (IR2 * Critical Infrastructure Impact2) + (IR3 * Critical Infrastructure Impact3)

Definition of Terms Specific to the Expression ROI # 1

Savings: = (Resistance Savings + Recognition Savings + Reconstitution Savings)

Resistance Savings
SR1: = IR1 * (Cleanup1 + Lost Opportunity1 + Critical Infrastructure Impact1)

Recognition Savings
SR2: = IR2 * (Cleanup2 + Lost Opportunity2 + Critical Infrastructure Impact2)

Reconstitution Savings
SR3: = IR3 * (Cleanup3 + Lost Opportunity3 + Critical Infrastructure Impact3)

Dud Costs
SR4: = IR4 * (Cleanup4)

Definition of Terms Specific to the Expressions ROI #2 and ROI # 3

Incidents Impacting: = Expected number of incidents not handled
IN3: Number of expected incidents not successfully survived
IN4: Number of expected incidents undetected (duds) except for a forensic trace
Full Cost Incurred: = (Full Cleanup + Full Lost Opportunity + Full Critical Infrastructure)
Cost with Avoidance: = (Reduced Cleanup + Reduced Lost Opportunity + Reduced Critical Infrastructure)

Computing the Terms in Security ROI Expressions

Based on initializing the security ROI model, we can compute the terms in security ROI expressions and prepare examples of ROI #1, ROI #2, and ROI #3.

Initializing the Security ROI Model

The number of expected incidents is set at 100, allocated as follows:

- Resistance 60
- Recognition 30
- Reconstitution 5
- Duds 5

The number of expected incidents impacting is set at 100, allocated as follows:

- Resistance 0
- Recognition 0
- Reconstitution 50
- Duds 50

Readiness preparation effort occurs in five steps as follows:

1. Step 1: Awareness & Commitment [number of days * number of participants * cost per day] = [3 * 50 * 500] = $75,000
2. Step 2: Basic Practices Training [number of days * number of participants * cost per day] = [5 * 25 * 600] = $75,000
3. Step 3: = Resistance and Recognition implementation costs $250,000
4. Step 4: = Reconstitution implementation costs $500,000
5. tep 5: = Information disclosure control costs $50,000

Cleanup costs, a function of incident types, are distinguished by resistance, recognition, and reconstitution as follows:

- Resistance: $2,500 per incident
- Recognition: $25,000 per incident
- Reconstitution: $250,000 per incident
- Dud: $250 per incident

Lost opportunity costs per incident are a function of incident type. They are distinguished by resistance, recognition, and reconstitution as follows:

- Resistance: [number of days * lost opportunity cost/day for incidents successfully survived] = [0.1 * 100000] = $10,000
- Recognition: [number of days * lost opportunity cost/day for incidents successfully survived] = [0.2 * 100000] = $20,000
- Reconstitution: [number of days * lost opportunity cost/day for incidents successfully survived] = [5 * 100000] = $500,000

Critical infrastructure costs per incident are associated with the number of days system services are unavailable as follows:

- Reconstitution: [number of days * lost opportunity cost/day for incidents successfully resisted] = [5 * $1000000] = $5,000,000

Examples of Calculations for ROI#1, ROI#2, and ROI#3

In this section, we provide brief examples of the calculations for ROI #1, ROI #2, and ROI #3. Complete examples for ROI #1, ROI #2, and ROI #3 can be found in the Appendix[6].

As noted in other BSI business case articles, there is very little actual public ROI data. An exception is the return on security investment work performed by the Hoover project [Soo Hoo 01[7]]. Owing to the dearth of actual data, this analysis is based on example numbers of incidents (as listed in the section on initializing our model). It is our hope that BSI readers will try a variety of techniques to compute security ROI, so that the various approaches presented can be validated in the future.

Example Calculation for ROI #1

Savings: = (Resistance Savings + Recognition Savings + Reconstitution Savings)
Cost: = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical Infrastructure Impact)
Savings: = 750,000 + 1,350,000 + 28,750,000) = 30,850,000
Cost: = (950,000 + 2,151,250 + 3,700,000 + 25,000,000) = 31,801,250
ROI: = Savings/Cost
ROI: = 30,850,000/31,801,250
ROI: = 0.97008765379

Example: ROI #2

Savings: = (Full Cost Incurred # Cost with Avoidance)
Cost: = (Total Preparation + Cost with Avoidance)
Savings: = (Full Cost Incurred – Cost with Avoidance)
Savings: = 287,512,500 # 30,851,250 = 256,661,250
Cost: = (Total Preparation + Cost with Avoidance)
Cost: = 950,000 + 30,851,250 = 31,801,250
ROI: = Savings/Cost
ROI: = 256,661,250/31,801,250
ROI: = 8.0707912425

6. #dsy677-BSI_Appendix
7. #dsy677-BSI_soohoo01

Example: ROI #3

Savings: = (Full Cost Incurred)
Cost: = (Total Preparation + Cost with Avoidance)
Savings: = (Full Cost Incurred)
Savings: = 287,512,500
Cost: = (Total Preparation + Cost with Avoidance)
Cost: = 950,000 + 30,851,250 = 31,801,250
ROI: = Savings/Cost
ROI: = 287,512,500/31,801,250
ROI: = 9.0409182029

Analyzing Security Return on Investment Results

Populating the terms of the security ROI expressions and analyzing the results uncover the behaviors of the drivers of security cost and savings. The computation of the security ROI suggests that the investment costs in readiness preparation produce only a marginal impact on security ROI (Figure 1[8]).

To evaluate security ROI expressions for your enterprise, visit the Security Return on Investment Interactive Worksheet tool[9] [O'Neill 06[10]].

Figure 1: Computing security ROI: analysis findings

Security Return on Investment - 10 Incidents				
	Fully Populated	W/O Critical Infra	W/O Lost Opportunity	W/O Critical and Lost
ROI #1	0.76453641461	0.38107645957	0.74076600389	0.18452955691
ROI #2	6.360676559	2.0624541975	6.4216431909	0.88928226585
ROI #3	7.1252439516	2.4436120837	7.1624433	1.0739191074
Security Return on Investment - 50 Incidents				
	Fully Populated	W/O Critical Infra	W/O Lost Opportunity	W/O Critical and Lost
ROI #1	0.94194878058	0.75471698113	0.93455531173	0.53070040111
ROI #2	7.8366856227	4.0846637639	8.1015877114	2.5575439679
ROI #3	8.7786725697	4.8395420094	9.0361860505	3.0885529158
Security Return on Investment - 100 Incidents				
	Fully Populated	W/O Critical Infra	W/O Lost Opportunity	W/O Critical and Lost
ROI #1	0.97008765379	0.86013600441	0.96614919265	0.69326884321
ROI #2	8.0707912425	4.6552104393	8.3754726213	3.3409915357
ROI #3	9.0409182029	5.5155302334	9.341666296	4.0346634422
Security Return on Investment - 1000 Incidents				
	Fully Populated	W/O Critical Infra	W/O Lost Opportunity	W/O Critical and Lost
ROI #1	0.99688976855	0.98381332773	0.99646740377	0.9571508069
ROI #2	8.2937754978	5.3245743115	8.6382988485	4.612687813
ROI #3	9.290705659	6.3085978558	9.6348121301	5.5703951029

The critical infrastructure impact is the dominant term in the security ROI expression; it is reflected in Figure 1[13] under the headings "W/O Critical Infra" and "W/O Critical and Lost." The lost opportunity is the second most dominant term in computing security ROI; it is reflected in Figure 1[14] under the headings "W/O Lost Opportunity" and "W/O Critical and Lost." For analysis purposes, each security ROI method is computed

8. #dsy677-BSI_figure1
9. http://members.aol.com/ONeillDon2/sec-roi_frames.html
10. #dsy677-BSI_oneill06
13. #dsy677-BSI_figure1
14. #dsy677-BSI_figure1

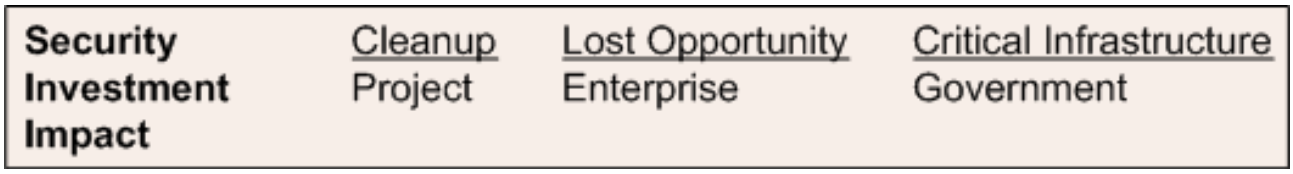
fully populated for all terms. Then each dominant term is excluded, and finally both dominant terms are excluded.

Analysis findings lead to the following conclusions:

- An organization expecting to experience a very low number of cyber attack incidents (10) may not recoup its security readiness investment unless both lost opportunity and critical infrastructure cost avoidance are included.
- An organization expecting to experience at least a low to moderate number of cyber attack incidents (50 or more) should expect to recoup its security readiness investment cost even if either lost opportunity or critical infrastructure cost avoidance is excluded.
- An organization expecting to experience a high number of cyber attack incidents (100 or more) should expect to recoup its security readiness investment cost through cleanup even if both lost opportunity and critical infrastructure cost avoidance are excluded.

Note that the estimated number of cyber attack incidents is very conservative and for illustration only. In reality, any organization with an Internet presence is likely to see more than 100 incidents. In a broader conclusion, the analysis suggests the recommendation that the cost burden for cleanup impact falls on the project, lost opportunity impact falls on the enterprise, and the cost burden for critical infrastructure impact falls on the government perhaps through insurance mechanisms (Figure 2[15]).

Figure 2: Security investment impact



Terminology

Survivability

Survivability spans the resistance to cyber attack, the recognition of a cyber attack, and the reconstitution of enterprise software operations following a cyber threat or cyber attack. The Software Engineering Institute (SEI) defines survivability “as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents.” The SEI identifies the key properties of survivable systems as resistance to attacks, recognition of attacks and the extent of damage, recovery of full and essential service after attack, and adaptation and evolution to reduce effectiveness of future attacks [Ellison 97[18]]. Survivability is achieved through the right blend of function, form, and fit. Software practices that result in highly secure and survivable software products may benefit security at the expense of competitiveness.

The survivability indicators are

- resistance (centers around improving the software infrastructure)
- recognition (revolves around sharing information on threats)
- reconstitution (centers around ensuring continuous operations, switching over, and restarting critical operations)

Appendix: Worked ROI Examples

A Worked Example: ROI #1

Savings: = (Resistance Savings + Recognition Savings + Reconstitution Savings)

15. #dsy677-BSI_figure2
18. #dsy677-BSI_ellison97

Cost: = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical Infrastructure Impact)

Where:

Incidents: = 100 [Expected number of incidents]
IR1: Number of expected incidents successfully resisted = 60
IR2: Number of expected incidents successfully recognized = 30
IR3: Number of expected incidents successfully survived = 5
IR4: Number of expected incidents undetected (duds) except for a forensic trace = 5

Resistance Savings
SR1: = IR1 * (Cleanup1 + Lost Opportunity1 + Critical Infrastructure Impact1)
SR1: = 60 * (2,500 + 10,000 + 0) = 750,000

Recognition Savings
SR2: = IR2 * (Cleanup2 + Lost Opportunity2 + Critical Infrastructure Impact2)
SR2: = 30 * (25,000 + 20,000 + 0) = 1,350,000

Reconstitution Savings
SR3: = IR3 * (Cleanup3 + Lost Opportunity3 + Critical Infrastructure Impact3)
SR3: = 5 * (250,000 + 500,000 +5,000,000) = 28,750,000

Dud Costs
SR4: = IR4 * (Cleanup4)
SR4: = 5 * (250) = 1,250

Preparation
Step 1: = 75,000 [3 days * 50 participants * $500/day]
Step 2: = 75,000 [5 days * 25 participants * $600/day]
Step 3: = 250,000 [Resistance and Recognition implementation costs]
Step 4: = 500,000 [Reconstitution implementation costs]
Step 5: = 50,000 [Information disclosure control costs]
Total Preparation: = (Step1 + Step2 + Step3 + Step4 + Step5)
Total Preparation: = (75,000 + 75,000+ 250,000 + 500,000 + 50,000)
Total Preparation: = 950,000

Cleanup Per Incident
Cleanup1: = [2,500/incident]
Cleanup2: = [25,000/incident]
Cleanup3: = [250,000/incident]
Cleanup4: = [250/incident]
Total Cleanup: = (IR1 * Cleanup1) + (IR2 * Cleanup2) + (IR3 * Cleanup3) + (IR4 * Cleanup4)
Total Cleanup: = (60 * 2,500) + (30 * 25,000) + (5* 250,000) + (5 * 250) = 150,000 + 750,000 + 1,250,000 + 1,250
Total Cleanup: = 2,151,250

Lost Opportunity Per Incident
Lost Opportunity1:= 0.1 day * 10,000/day: = 10,000
Lost Opportunity2:= 0.2 days * 10,000/day: = 20,000
Lost Opportunity3:= 5 days * 100,000/day:= 500,000
Total Lost Opportunity: = (IR1 * Lost Opportunity1) + (IR2 * Lost Opportunity2) + (IR3 * Lost Opportunity3)
Total Lost Opportunity: = (60 * 10,000) + (30 * 20,000) + (5 *500,000)
Total Opportunity: = 600,000 + 600,000 + 2,500,000
Total Lost Opportunity: = 3,700,000

Critical Infrastructure Impact Per Incident
Critical Infrastructure Impact1:= 0 * 1,000,000:= 0
Critical Infrastructure Impact2:= 0 * 1,000,000:= 0

Critical Infrastructure Impact3:= 5 * 1,000,000:= 5,000,000
Total Critical Infrastructure Impact: = (60 * 0) + (30 * 0) + (5* 5,000,000): = 25,000,000
Savings: = (Resistance Savings + Recognition Savings + Reconstitution Savings)
Cost: = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical Infrastructure Impact)
Savings: = 750,000 + 1,350,000 + 28,750,000) = 30,850,000
Cost: = (950,000 + 2,151,250 + 3,700,000 + 25,000,000) = 31,801,250
ROI: = Savings/Cost
ROI: = 30,850,000/31,801,250
ROI: = 0.97008765379

A Worked Example: ROI #2

Savings: = (Full Cost Incurred # Cost with Avoidance)
Cost: = (Total Preparation + Cost with Avoidance)

Where:
Incidents: = Expected number of incidents
IR1: Number of expected incidents successfully resisted = 60
IR2: Number of expected incidents successfully recognized = 30
IR3: Number of expected incidents successfully survived = 5
IR4: Number of expected incidents undetected (duds) except for a forensic trace = 5
Incidents Impacting: = Expected number of incidents not handled
IN3: Number of expected incidents not successfully survived = 50
IN4: Number of expected incidents undetected (duds) except for a forensic trace = 50
Full Cost Incurred: = (Full Cleanup + Full Lost Opportunity + Full Critical Infrastructure) = (12,512,500 + 25,000,000 + 250,000,000) = 287,512,500
Cost with Avoidance: = (Reduced Cleanup + Reduced Lost Opportunity + Reduced Critical Infrastructure) = (2,151,250 + 3,700,000 + 25,000,000) = 30,851,250

Preparation
Step 1: = 75,000 [3 days * 50 participants * $500/day]
Step 2: = 75,000 [5 days * 25 participants * $600/day]
Step 3: = 250,000 [Resistance and Recognition implementation costs]
Step 4: = 500,000 [Reconstitution implementation costs]
Step 5: = 50,000 [Information disclosure control costs]
Total Preparation: = (Step1 + Step2 + Step3 + Step4 + Step5)
Total Preparation: = (75,000 + 75,000+ 250,000 + 500,000 + 50,000)
Total Preparation: = 950,000

Cleanup Per Incident
Cleanup1: = Cost/incident for incidents successfully resisted = 2500
Cleanup2: = Cost/incident for incidents successfully recognized= 25,000
Cleanup3: = Cost/incident for incidents successfully survived = 250,000
Cleanup4: = Cost/incident for incidents undetected (duds) except for a forensic trace = 250
Total Cleanup: = (IR1 * Cleanup1) + (IR2 * Cleanup2) + (IR3 * Cleanup3) + (IR4 * Cleanup4)
Full Cleanup: = (IN3 * Cleanup3) + (IN4 * Cleanup4)
Full Cleanup: = 50 * 250,000 + 50 * 250 = 12,512,500
Reduced Cleanup: = (IR1 * Cleanup1) + (IR2 * Cleanup2) + (IR3 * Cleanup3) + (IR4 * Cleanup4)
Reduced Cleanup: = (60 * 2,500) + (30 * 25,000) + (5* 250,000) + (5 * 250) = 150,000 + 750,000 + 1,250,000 + 1,250 = 2,151,250

Lost Opportunity Per Incident
Lost Opportunity1: = number of days * lost opportunity cost/day for incidents successfully resisted = 0.1 * 100,000 = 10,000
Lost Opportunity2: = number of days * lost opportunity cost/day for incidents successfully recognized = 0.2 * 100,000 = 20,000

Lost Opportunity3: = number of days * lost opportunity cost/day for incidents successfully survived = 5 * 100,000 = 500,000
Total Lost Opportunity: = (IR1 * Lost Opportunity1) + (IR2 * Lost Opportunity2) + (IR3 * Lost Opportunity3)
Full Lost Opportunity: = (IN3 * Lost Opportunity3)
Full Lost Opportunity: = 50 * 500,000 = 25,000,000
Reduced Lost Opportunity: = (IR1 * Lost Opportunity1) + (IR2 * Lost Opportunity2) + (IR3 * Lost Opportunity3)
Reduced Lost Opportunity: = (60 * 10,000) + (30 * 20,000) + (5 * 500,000) = 600,000 + 6,000,000 + 2,500,000 = 3,700,000

Critical Infrastructure Impact Per Incident
Critical Infrastructure Impact1: = number of days * lost opportunity cost/day for incidents successfully resisted = 0 * 1,000,000 = 0
Critical Infrastructure Impact2: = number of days * lost opportunity cost/day for incidents successfully recognized = 0 * 1,000,000 = 0
Critical Infrastructure Impact3: = number of days * lost opportunity cost/day for incidents successfully survived = 5 * 1,000,000 = 5,000,000
Total Critical Infrastructure Impact: = (IR1 * Critical Infrastructure Impact1) + (IR2 * Critical Infrastructure Impact2) + (IR3 * Critical Infrastructure Impact3)
Total Critical Infrastructure Impact: = (60 * 0) + (30 * 0) + (5* 5,000,000): = 25,000,000
Full Critical Infrastructure: = (IN1 * Critical Infrastructure Impact1) + (IN2 * Critical Infrastructure Impact2) + (IN3 * Critical Infrastructure Impact3)
Full Critical Infrastructure: = (60 * 0) + (30 * 0) + (50 * 5,000,000) = 2,500,000,000
Reduced Critical Infrastructure: = (IR1 * Critical Infrastructure Impact1) + (IR2 * Critical Infrastructure Impact2) + (IR3 * Critical Infrastructure Impact3)
Reduced Critical Infrastructure: = (60 * 0) + (30 * 0) + (5 * 5,000,000) = 25,000,000
Savings: = (Full Cost Incurred # Cost with Avoidance)
Cost: = (Total Preparation + Cost with Avoidance)
Savings: = (Full Cost Incurred # Cost with Avoidance) = 287,512,500 # 30,851,250 = 256,661,250
Cost: = (Total Preparation + Cost with Avoidance) = 950,000 + 30,851,250 = 31,801,250
ROI: = Savings/Cost
ROI: = 256,661,250/31,801,250
ROI: = 8.0707912425

A Worked Example: ROI #3

Savings: = (Full Cost Incurred)
Cost: = (Total Preparation + Cost with Avoidance)

Where:
Incidents: = Expected number of incidents
IR1: Number of expected incidents successfully resisted = 60
IR2: Number of expected incidents successfully recognized = 30
IR3: Number of expected incidents successfully survived = 5
IR4: Number of expected incidents undetected (duds) except for a forensic trace = 5
Incidents Impacting: = Expected number of incidents not handled
IN3: Number of expected incidents not successfully survived = 50
IN4: Number of expected incidents undetected (duds) except for a forensic trace = 50
Full Cost Incurred: = (Full Cleanup + Full Lost Opportunity + Full Critical Infrastructure) = (12,512,500 + 25,000,000 + 250,000,000) = 287,512,500
Cost with Avoidance: = (Reduced Cleanup + Reduced Lost Opportunity + Reduced Critical Infrastructure) = (2,151,250 + 3,700,000 + 25,000,000) = 30,851,250

Preparation
Step 1: = 75,000 [3 days * 50 participants * $500/day]

Step 2: = 75,000 [5 days * 25 participants * $600/day]
Step 3: = 250,000 [Resistance and Recognition implementation costs]
Step 4: = 500,000 [Reconstitution implementation costs]
Step 5: = 50,000 [Information disclosure control costs]
Total Preparation: = (Step1 + Step2 + Step3 + Step4 + Step5)
Total Preparation: = (75,000 + 75,000+ 250,000 + 500,000 + 50,000)
Total Preparation: = 950,000

Cleanup Per Incident
Cleanup1: = cost/incident for incidents successfully resisted = 2,500
Cleanup2: = cost/incident for incidents successfully recognized = 25,000
Cleanup3: = cost/incident for incidents successfully survived = 250,000
Cleanup4: = cost/incident for incidents undetected (duds) except for a forensic trace = 250
Total Cleanup: = (IR1 * Cleanup1) + (IR2 * Cleanup2) + (IR3 * Cleanup3) + (IR4 * Cleanup4)
Full Cleanup: = (IN3 * Cleanup3) + (IN4 * Cleanup4)
Full Cleanup: = 50 * 250,000 + 50 * 250 = 12,512,500
Reduced Cleanup: = (IR1 * Cleanup1) + (IR2 * Cleanup2) + (IR3 * Cleanup3) + (IR4 * Cleanup4)
Reduced Cleanup: = (60 * 2,500) + (30 * 25,000) + (5* 250,000) + (5 * 250) = 150,000 + 750,000 + 1,250,000 + 1,250 = 2,151,250

Lost Opportunity Per Incident
Lost Opportunity1: = number of days * lost opportunity cost/day for incidents successfully resisted = 0.1 * 100,000 = 10,000
Lost Opportunity2: = number of days * lost opportunity cost/day for incidents successfully recognized = 0.2 * 100,000 = 20,000
Lost Opportunity3: = number of days * lost opportunity cost/day for incidents successfully survived = 5 * 100,000 = 500,000
Total Lost Opportunity: = (IR1 * Lost Opportunity1) + (IR2 * Lost Opportunity2) + (IR3 * Lost Opportunity3)
Full Lost Opportunity: = (IN3 * Lost Opportunity3)
Full Lost Opportunity: = 50 * 500,000 = 25,000,000
Reduced Lost Opportunity: = (IR1 * Lost Opportunity1) + (IR2 * Lost Opportunity2) + (IR3 * Lost Opportunity3)
Reduced Lost Opportunity: = (60 * 10,000) + (30 * 20,000) + (5 * 500,000) = 600,000 + 6,000,000 + 2,500,000 = 3,700,000

Critical Infrastructure Impact Per Incident
Critical Infrastructure Impact1: = number of days * lost opportunity cost/day for incidents successfully resisted = 0 * 1,000,000 = 0
Critical Infrastructure Impact2: = number of days * lost opportunity cost/day for incidents successfully recognized = 0 * 1,000,000 = 0
Critical Infrastructure Impact3: = number of days * lost opportunity cost/day for incidents successfully survived = 5 * 1,000,000 = 5,000,000
Total Critical Infrastructure Impact: = (IR1 * Critical Infrastructure Impact1) + (IR2 * Critical Infrastructure Impact2) + (IR3 * Critical Infrastructure Impact3)
Total Critical Infrastructure Impact: = (60 * 0) + (30 * 0) + (5* 5,000,000):= 25,000,000
Full Critical Infrastructure: = (IN1 * Critical Infrastructure Impact1) + (IN2 * Critical Infrastructure Impact2) + (IN3 * Critical Infrastructure Impact3)
Full Critical Infrastructure: = (60 * 0) + (30 * 0) + (50 * 5,000,000) = 2,500,000,000
Reduced Critical Infrastructure: = (IR1 * Critical Infrastructure Impact1) + (IR2 * Critical Infrastructure Impact2) + (IR3 * Critical Infrastructure Impact3)
Reduced Critical Infrastructure: = (60 * 0) + (30 * 0) + (5 * 5,000,000) = 25,000,000
Savings: = (Full Cost Incurred)
Cost: = (Total Preparation + Cost with Avoidance)
Savings: = (Full Cost Incurred) = 287,512,500

Cost: = (Total Preparation + Cost with Avoidance) = 950,000 + 30,851,250 = 31,801,250
ROI: = Savings/Cost
ROI: = 287,512,500/31,801,250
ROI: = 9.0409182029

References

[Arora 04]	Arora, A.; Hall, D.; Piato, C. A.; Ramsey, D.; & Telang, R. "Measuring the Risk-Based Value of IT Security Solutions." *IEEE IT Professional 6*, 6 (Nov.-Dec. 2004): 35-42.
[Arora 05]	Arora, A.; Frank, Steven; & Telang, Rahul. *Estimating Benefits from Investing in Secure Software Development*[19]. (2005).
[Ellison 97]	Ellison, B.; Fisher, D. A.; Linger, R. C.; Lipson, H. F.; Longstaff, T.; & Mead, N. R. *Survivable Network Systems: An Emerging Discipline*[20] (CMU/SEI-97-TR-013, ADA341963). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1997.
[O'Neill 03]	O'Neill, Don. "Security Return on Investment[21]." *The Competitor 6*, 4 (March 2003).
[SooHoo 01]	Soo Hoo, K.; Sudbury, A. W.; & Jaquith, A. R. "Tangible ROI through Secure Software Engineering." *Secure Business Quarterly 1*, 2 (Fourth Quarter 2001).

Tools

[O'Neill 06]	O'Neill, Don, "Security Return on Investment Interactive Worksheet[22]."

Carnegie Mellon Copyright

1. mailto:permission@sei.cmu.edu